

Amendments to the Claims:

1. (Currently Amended) A ~~public, non-commutative~~ method for ~~encoding-encrypting~~ an original message to be passed to a recipient by way of an grantor, the method comprising the steps of:

obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor according to a public key encryption scheme;

generating a public proxy key based on a private key corresponding to the recipient and on the private key corresponding to said grantor, wherein said grantor's private key and said recipient's private key are combined, and the combination of the private keys is based on said public key encryption scheme and provides that ,wherein it is computationally difficult to recover the recipient's private key corresponding to the recipient from the public proxy key even with the knowledge of the grantor's private key; and

applying the public proxy key to transform the encrypted message into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient and ~~any-the~~ available public key information.

2. (Original) The method of claim 1, wherein the encrypted message has been encrypted with an ElGamal encryption scheme.

3. (Original) The method of claim 1, wherein the encrypted message has been encrypted with a modified ElGamal encryption scheme.

4. (Original) The method of claim 1, wherein the receiving, generating, and applying steps are performed by the grantor.

5. (Original) The method of claim 1, further comprising the step of providing the transformed message to the recipient.

6. (Original) The method of claim 5, further comprising the step of decrypting the transformed message using information selected from the private key corresponding to the recipient and any available public information.

7. (Original) The method of claim 5, further comprising the step of decrypting the transformed message using the private key corresponding to the recipient.

8. (Original) The method of claim 2, wherein the encrypted message comprises a first portion and a second portion, the first portion encoding a generator and a random key, and the second portion encoding the original message, the public key corresponding to the grantor, and the random key.

9. (Original) The method of claim 8, wherein the applying step operates on the second portion of the encrypted message.

10. (Original) The method of claim 3, wherein the encrypted message comprises a first portion and a second portion, the first portion encoding the original message, a generator, and a random key, and the second portion encoding the public key corresponding to the grantor and the random key.

11. (Original) The method of claim 10, wherein the applying step operates on the second portion of the encrypted message.

12. (Original) The method of claim 4, wherein the encrypted message comprises a first portion and a second portion, the first portion encoding the original message, a generator, and a random key, and the second portion encoding the public key corresponding

to the grantor and the random key.

13. (Original) The method of claim 12, wherein the applying step operates on the second portion of the encrypted message.

14. (Original) The method of claim 1, wherein the original message is passed to a recipient through at least one additional intermediate grantor by repeating the generating and applying steps for each additional intermediate grantor.

15. (Currently Amended) A ~~public, non-commutative~~ method for encrypting an original message to be passed to a recipient by way of an grantor, the method comprising the steps of:

obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor according to a public key encryption scheme;

generating a public proxy key based on a public key corresponding to the recipient and on the private key corresponding to the public key of said grantor, wherein said grantor's private key and said recipient's public key are combined, and the combination of said grantor's private key and said recipient's public key is based on said public key encryption scheme; and

applying the public proxy key to transform the encrypted message ~~transforming the encrypted message, using a transformation key corresponding to the recipient,~~ into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from a the private key corresponding to the recipient recipient's public key and any the available public key information.

16-17. (Canceled)

18. (Original) The method of claim 15, wherein the encrypted message has been

encrypted with a Cramer-Shoup encryption scheme.

19. (Original) The method of claim 15 wherein the transformed message is decryptable by the recipient using a private key corresponding to the recipient.

20. (Currently Amended) The method of claim 15, wherein the original message is passed to a recipient through at least one additional intermediate grantor by repeating the steps of generating and applying transforming step for each additional intermediate grantor.

21. (New) The method of claim 15 wherein it is computationally difficult to recover the grantor's private key from the public proxy key.

22. (New) The method of claim 15, wherein the encrypted message has been encrypted with an ElGamal encryption scheme.

23. (New) The method of claim 15, wherein the encrypted message has been encrypted with a modified ElGamal encryption scheme.

24. (New) The method of claim 15, wherein the receiving, generating, and applying steps are performed by the grantor.

25. (New) The method of claim 24, further comprising a step of obtaining said recipient's private key by said grantor.

26. (New) The method of claim 1, wherein the encrypted message has been encrypted with a Cramer-Shoup encryption scheme.

27. (New) The method of claim 1, wherein it is computationally difficult to recover the grantor's private key from the public proxy key.

ATTORNEY DOCKET NO.: 111325-006 (040100)

Application No.: 09/468,703

Page 6

28. (New) The method of claim 1, wherein said public encryption scheme is a discrete-logarithm-based encryption scheme, wherein said combination of said private keys comprises using the modular difference of both private keys as an exponent in a modular exponentiation.

29. (New) The method of claim 4, further comprising a step of obtaining the recipient's private key by the grantor.